

Recap : a group is given by

- set G
- binary op. $* : G \times G \rightarrow G$ (i.e. $a, b \in G \Rightarrow a * b \in G$)
- s.t. - there is an/the identity elem. $e \in G$
 $e * a = a = a * e$
- each $a \in G$ has its inverse $a^{-1} \in G$
 $a * a^{-1} = e = a^{-1} * a$

Convention

- we often say " G is a group" to mean it has an bin. op. $*$ as above
- we often use "multiplicative notation" ab for $a * b$

$\underbrace{a a \dots a}_{n \text{ times}}$ denoted by a^n , $\underbrace{a^{-1} \dots a^{-1}}_{n \text{ times}}$ by a^{-n}

so $a^m a^n = a^{m+n}$ with $a^0 = e$

- write $a + b$ if $*$ should be interpreted as "addition of a and b " (then $a + b = b + a, \dots$)

write na for $\underbrace{a + \dots + a}_{n \text{ times}}$

§5 Subgroups

We often consider "subsystems" of a group:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \dots$ inside $\mathbb{C}$ for addition as group bin. op.
- $SO(3) = \{X \in M_3 \mid X^T X = I_3, \det X = 1\} \subset GL_3$
 rotation group invertible 3×3 matrixes

A subgroup of a group $(G, *)$ is given by

a subset $H \subset G$ s.t. $a, b \in H \Rightarrow a * b, a^{-1} \in H$
 $e \in H$

so $(H, \text{restr. of } * \text{ to } H \times H)$ becomes a group

(Def. 5.4, Thm. 5.14)

Some quick examples

- we allow $H = G$ as a subgroup

- $H = \{e\}$ is always a subgroup $e * e = e, e^{-1} = e$

$$a * (e * e) = (a * e) * e = a * e = a$$

$$a * e^{-1} = a \quad \text{from} \quad b^{-1} * e^{-1} = (e * b)^{-1} = b^{-1}$$

(use this for $b^{-1} = a \Leftrightarrow b = a^{-1}$)

Cyclic (sub)groups

fix a group G (we write ab for the bin. op.)

and an element $a \in G$

Thm 5.17 The subset $\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$
 $= \{ \underbrace{a \cdots a}_{n \text{ times}}, e, \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ times}} \mid n = 1, 2, \dots \}$

of G is a subgroup of G

Proof we need to check $a^m a^n, (a^m)^{-1}, e$ are elements of $\langle a \rangle$ for all $m, n \in \mathbb{Z}$

- $a^m a^n$: use $a^m a^n = a^{m+n}$

- $(a^m)^{-1}$: check $(a^m)^{-1} = a^{-m}$ by computing

$$a^m a^{-m} = e = a^{-m} a^m$$

$$\text{if } m > 0 \quad a^m a^{-m} = \underbrace{a \cdots a}_{m \text{ times}} \underbrace{a^{-1} \cdots a^{-1}}_{m \text{ times}}$$

use $a a^{-1} = e$ in the middle, then $a e = a$

to remove e , repeat this argument ~~the~~

$$\text{if } m = 0 \quad a^m a^{-m} = a^0 a^0 = e e = e$$

by conv.

$$\text{if } m < 0 \quad a^m a^{-m} = a^{-1} \cdots a^{-1} a \cdots a$$

use $a^{-1} a = e$ and use a similar arg.

as above $\square$

We call $\langle a \rangle$ the cyclic subgroup of G generated by a

We have two cases:

- the elements a^n ($n \in \mathbb{Z}$) are all distinct

ex. $G = \mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$ with multiplication as group bin. op.

and $a \neq 1$

$\rightarrow (\mathbb{Z}, +) \xrightarrow{\phi} (\langle a \rangle, \cdot)$, $n \mapsto a^n$ is an isomorphism
($\phi(n) = a^n$)

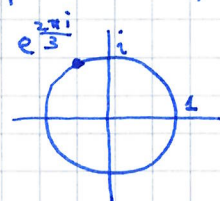
$$\rightarrow a^{n+k} = a^n$$

- there are some nonzero integers k s.t. $a^k = e$

ex. $G = \mathbb{C}^\times = \{z \in \mathbb{C} \mid z \neq 0\}$ with mult. as group bin. op.

$$a = e^{\frac{2\pi i}{m}} = \cos \frac{2\pi}{m} + i \sin \frac{2\pi}{m}$$

satisfies $a^m = 1 = e$



ex. $G = \mathbb{Z}_m = \{\text{integers up to congruence modulo } m\}$
identify a, b if $a - b = km$ for some int. k

with addition as group bin. op.

and $a = 1$ $ma = m$ is identified with

$$0 = e$$

In general, take $m =$ smallest positive integer such that $a^m = e$

(call m the order of a in G)

Thm Then $a^l = e$ if and only if $l = km$ for some integer k

Proof "if" from $a^l = a^{km} = (a^m)^k = e^k = e$

"only if": Suppose $a^l = e$ we want $l = km$

Step 1 we may assume $l > 0$: $a^{-l} = (a^l)^{-1}$

Step 2 write $l = km + r$ $r = 0, 1, \dots, m-1$

we want $r = 0$ Argue by contradiction

$$a^r = a^l a^{-km} = e e^{-k} = e$$

if $r > 0$ this would violate the minimality of m

With m as above,

$(\mathbb{Z}_m, +) \xrightarrow{\phi} (\langle a \rangle, \cdot), \quad n \mapsto a^n$ is
an isomorphism